CLAIMS

1. Method of coding information symbols according to a code defined on a Galois field $\mathbf{F}_q$, where q is an integer greater than 2 and equal to a power of a prime number, and of length $n = p(q-1)$, where p is an integer greater than 1, characterized in that it comprises the following steps:

a) a p-tuple of integers $(t_1,\ldots,t_p)$ is chosen such that

$$q-1 > t_1 > t_2 > \ldots > t_p > 0,$$

and a p-tuple of diagonal square matrices $(Y_1,\ldots,Y_p)$ of dimension $(q-1)$ on $\mathbf{F}_q$ such that, for any i $(1 \le i \le q-1)$, the p elements in position (i,i) of these matrices $Y_1,\ldots,Y_p$ are different in pairs,

b) said information symbols are placed successively in p words $\underline{a}_l$ of length $(q-1-t_l)$ (where $l = 1,\ldots,p$),

c) words $\underline{u}_l$ (where $l = 1,\ldots,p$) are formed of length $(q-1)$, which constitute the components of the "precoded word" $\underline{u} = [\underline{u}_1\ \underline{u}_2\ \cdots\ \underline{u}_p]$, by supplementing the corresponding word $\underline{a}_l$ by means of redundant symbols so that $\underline{u}_l$ is orthogonal to the matrix $H^{(t_l)}$, where the matrices $H^{(t)}$ are defined by $H^{(t)}{}_{ij} = \gamma^{i(j-1)}$ $(1 \le i \le t,\ 1 \le j \le q-1)$, where γ is a symbol chosen from amongst the primitive elements of $\mathbf{F}_q$, and

d) a code word

$$\underline{v} = [\underline{v}_1\ \underline{v}_2\ \cdots\ \underline{v}_p]$$

is formed, where each word $\underline{v}_l$ $(l = 1,\ldots,p)$ is of length $(q-1)$, by resolving the system of equations

$$\begin{cases} \underline{v}_1 + \underline{v}_2 + \ldots + \underline{v}_p = \underline{u}_1\,, \\ \underline{v}_1 Y_1 + \underline{v}_2 Y_2 + \ldots + \underline{v}_p Y_p = \underline{u}_2\,, \\ \underline{v}_1 Y_1^2 + \underline{v}_2 Y_2^2 + \ldots + \underline{v}_p Y_p^2 = \underline{u}_3\,, \\ \qquad\qquad \cdots \\ \underline{v}_1 Y_1^{p-1} + \underline{v}_2 Y_2^{p-1} + \ldots + \underline{v}_p Y_p^{p-1} = \underline{u}_p\,. \end{cases}$$

2. Coding method according to Claim 1, characterized in that an algebraic equation in X and Y is considered such that, for any value γ^{i-1} ($i = 1,\ldots,q-1$) taken by X, said algebraic equation has p distinct solutions denoted $y_l(\gamma^{i-1})$ (where $l = 1,\ldots,p$), and in that the diagonal element in position (i,i) of each of said matrices Y_l is taken to be equal to $y_l(\gamma^{i-1})$.

3. Coding method according to Claim 1 or Claim 2, characterized in that each word $\underline{a}_l$ (where $l = 1,\ldots,p$) represents a respective approximation of resolution of an image coded at source.

4. Method of decoding received data resulting from the transmission of coded symbols according to Claim 1, characterized in that it comprises the following steps:

e) from the word received

$$\underline{r} = [\underline{r}_1\ \underline{r}_2 \cdots \underline{r}_p],$$

where each word $\underline{r}_l$ ($l = 1,\ldots,p$) is of length $(q-1)$, at least one of the components $\underline{s}_l$ (where $l = 1,\ldots,p$) of length $(q-1)$, of the "post-received word" $\underline{s} = [\underline{s}_1\ \underline{s}_2 \cdots \underline{s}_p]$, is calculated, according to:

$$\begin{cases} \underline{s}_1 = \underline{r}_1 + \underline{r}_2 + \ldots + \underline{r}_p, \\ \underline{s}_2 = \underline{r}_1 Y_1 + \underline{r}_2 Y_2 + \ldots + \underline{r}_p Y_p, \\ \underline{s}_3 = \underline{r}_1 Y_1^2 + \underline{r}_2 Y_2^2 + \ldots + \underline{r}_p Y_p^2, \\ \qquad \cdots \\ \underline{s}_p = \underline{r}_1 Y_1^{p-1} + \underline{r}_2 Y_2^{p-1} + \ldots + \underline{r}_p Y_p^{p-1}, \end{cases}$$

and

f) at least one of the components $\underline{\hat{u}}_l$ (where $l = 1,\ldots,p$) of length $(q-1)$, of the "post-associated word" $\underline{\hat{u}} = [\underline{\hat{u}}_1 \underline{\hat{u}}_2 \ldots \underline{\hat{u}}_p]$, is calculated, correcting the word $\underline{s}_l$ with the same l according to the error syndrome vector $H^{(t_l)} \cdot \underline{s}_l^{\mathrm{T}}$.

5. Method of decoding received data resulting from the transmission of coded symbols according to Claim 2, characterized in that it comprises the following steps:

e') a maximal error correction algorithm is applied to each received word $\underline{r}$, so as to obtain an estimation

$\underline{\hat{v}} = [\underline{\hat{v}}_1 \; \underline{\hat{v}}_2 \cdots \underline{\hat{v}}_p]$,

where each word $\underline{\hat{v}}_l$ (l = 1,...,p) is of length (q−1), of the corresponding transmitted word $\underline{v}$, and

f') at least one of the components $\underline{\hat{u}}_l$ (where l = 1,...,p), of length (q−1), of the "post-associated word" $\underline{\hat{u}} = [\underline{\hat{u}}_1 \underline{\hat{u}}_2 \cdots \underline{\hat{u}}_p]$, is calculated, according to:

$$\begin{cases} \underline{\hat{u}}_1 = \underline{\hat{v}}_1 + \underline{\hat{v}}_2 + \ldots + \underline{\hat{v}}_p, \\ \underline{\hat{u}}_2 = \underline{\hat{v}}_1 Y_1 + \underline{\hat{v}}_2 Y_2 + \ldots + \underline{\hat{v}}_p Y_p, \\ \underline{\hat{u}}_3 = \underline{\hat{v}}_1 Y^2_1 + \underline{\hat{v}}_2 Y^2_2 + \ldots + \underline{\hat{v}}_p Y^2_p, \\ \qquad \ldots \\ \underline{\hat{u}}_p = \underline{\hat{v}}_1 Y_1^{p-1} + \underline{\hat{v}}_2 Y_2^{p-1} + \ldots + \underline{\hat{v}}_p Y_p^{p-1}. \end{cases}$$

6. Method of decoding received data resulting from the transmission of coded symbols according to Claim 2, characterized in that it comprises a preliminary step consisting of choosing, for the current received word, between the steps of the method according to Claim 4 and the steps of the method according to Claim 5, according to predetermined criteria.

7. Method of decoding received data resulting from the transmission of coded symbols according to Claim 2, characterized in that, for any word received, an error correction algorithm according to Claim 4 is first of all implemented and in that, should this algorithm not succeed, it is declared that a non-correctable error has been detected.

8. Method of decoding received data resulting from the transmission of coded symbols according to Claim 2, characterized in that, for any word received, an error correction algorithm is first of all implemented according to Claim 4, and in that, should this algorithm not succeed, an error correction algorithm according to Claim 5 is then implemented.

9. Decoding method according to any one of Claims 4 to 8, characterized in that it also comprises the step consisting of obtaining estimated information symbols by removing from at least one component $\underline{\hat{u}}_l$ (l = 1,...,p) the symbols situated at the identical positions to the positions of the component

$\underline{u}_l$ with the same l of the corresponding precoded word $\underline{u}$, in which the redundant symbols were placed at step c) of the method according to Claim 1.

10. Method of communicating information symbols comprising the following steps:

1) said information symbols are coded in accordance with a coding method according to Claim 1, so as to form the code words $\underline{v} = \left(v^0, v^1, \ldots, v^{n-1}\right)$,

2) the symbols of each code word $\underline{v}$ are permuted so as to form a word to be transmitted

$$\underline{v}^* = \left(v^0, v^{q-1}, v^{2(q-1)}, \ldots, v^{(p-1)(q-1)}, v^1, v^q, v^{2q-1}, \ldots, v^{(p-1)(q-1)+1}, \ldots, v^{n-1}\right),$$

3) said word $\underline{v}^*$ is transmitted,

4) an interleaved word

$$\underline{r}^* = \left(r^0, r^{q-1}, r^{2(q-1)}, \ldots, r^{(p-1)(q-1)}, r^1, r^q, v^{2q-1}, \ldots, r^{(p-1)(q-1)+1}, \ldots, r^{n-1}\right),$$

corresponding to the word $\underline{v}^*$ is received,

5) the symbols of the interleaved word $\underline{r}^*$ are permuted so as to form a received word $\underline{r} = \left(r^0, r^1, \ldots, r^{n-1}\right)$, and

6) the received word $\underline{r}$ is decoded in accordance with a decoding method according to Claim 4 or Claim 5.

11. Device (102) for coding information symbols according to a code defined on a Galois field $\mathbf{F}_q$, where q is an integer greater than 2 and equal to a power of a prime number, and of length $n = p(q-1)$, where p is an integer greater than 1, characterized in that, a p-tuple of integers $(t_1,\ldots,t_p)$ such that

$$q-1 > t_1 > t_2 > \ldots > t_p > 0,$$

and a p-tuple of diagonal square matrices $(Y_1,\ldots,Y_p)$ of dimension $(q-1)$ on $\mathbf{F}_q$ such that, for any i $(1 \leq i \leq q-1)$, the p elements in position (i,i) of these matrices $Y_1,\ldots,Y_p$ are different in pairs, having been chosen, it is able to:

- place said information symbols successively in p words $\underline{a}_l$ of length $(q-1-t_l)$ (where $l = 1,\ldots,p$),

- form words $\underline{u}_l$ (where $l = 1,\ldots,p$) of length $(q-1)$, which constitute the components of the "precoded word" $\underline{u} = [\underline{u}_1\ \underline{u}_2\ \cdots\ \underline{u}_p]$, supplementing the

corresponding word $\underline{a}_l$ by means of redundant symbols so that $\underline{u}_l$ is orthogonal to the matrix $H^{(t_l)}$, where the matrices $H^{(t)}$ are defined by $H^{(t)}_{ij} = \gamma^{i(j-1)}$ ($1 \le i \le t$, $1 \le j \le q-1$), where γ is a symbol chosen from amongst the primitive elements of $\mathbf{F}_q$, and

- form a code word

$$\underline{v} = [\underline{v}_1\ \underline{v}_2\ \cdots\ \underline{v}_p],$$

where each word $\underline{v}_l$ ($l = 1,\ldots,p$) is of length ($q-1$), by resolving the system of equations

$$\begin{cases} \underline{v}_1 + \underline{v}_2 + \ldots + \underline{v}_p = \underline{u}_1, \\ \underline{v}_1 Y_1 + \underline{v}_2 Y_2 + \ldots + \underline{v}_p Y_p = \underline{u}_2, \\ \underline{v}_1 Y^2_1 + \underline{v}_2 Y^2_2 + \ldots + \underline{v}_p Y^2_p = \underline{u}_3, \\ \qquad\ldots \\ \underline{v}_1 Y_1^{p-1} + \underline{v}_2 Y_2^{p-1} + \ldots + \underline{v}_p Y_p^{p-1} = \underline{u}_p. \end{cases}$$

12. Coding device according to Claim 11, characterized in that it is also able to assign the value $y_l(\gamma^{i-1})$ to the diagonal element in position (i,i) of each of said matrices Y_l, where, for a predetermined algebraic equation in X and Y, said algebraic equation has p distinct solutions denoted $y_l(\gamma^{i-1})$ (where $l = 1,\ldots,p$) for any value γ^{i-1} ($i = 1,\ldots,q-1$) taken by X.

13. Device (10) for decoding received words $\underline{r}$ resulting from the transmission of coded words $\underline{v}$ according to the invention, characterized in that it comprises:

- an error correction unit (107) able to apply an error correction algorithm to each word received $\underline{r}$, so as to supply at least one component $\underline{\hat{u}}_l$ (where $l = 1,\ldots,p$) of a "post-associated word" $\underline{\hat{u}}$, and

- a redundancy elimination unit (108) able to remove from said component $\underline{\hat{u}}_l$ the symbols situated at the positions identical to the positions of the component $\underline{u}_l$ with the same l of the corresponding precoded word $\underline{u}$, in which redundant symbols were placed at the time of coding.

14. Device for decoding received words $\underline{r}$ resulting from the transmission of coded words $\underline{v}$ according to Claim 2, characterized in that it comprises:

- a selection unit (40) capable of determining, according to predetermined criteria, whether it is necessary to apply to the current received word $\underline{r}$ the steps of the method according to Claim 4 and/or the steps of the method according to Claim 5,

- an error correction unit (107) able to apply an error correction algorithm to each received word $\underline{r}$, so as to supply at least one component $\underline{\hat{u}}_l$ (where $l = 1,\ldots,p$) of a "post-associated word" $\underline{\hat{u}}$, and

- a redundancy elimination unit (108) able to remove from said component $\underline{\hat{u}}_l$ the symbols situated at the identical positions to the positions of the component $\underline{u}_l$ of the same l of the corresponding precoded word $\underline{u}$ in which redundant symbols were placed during coding.

15. Information data transmission apparatus (48), characterized in that it comprises a coding device according to Claim 11 or Claim 12, as well as a modulator (103) for modulating the data resulting from the coding of said information data.

16. Data reception apparatus (70), characterized in that it comprises a demodulator (106) for demodulating the received data, as well as a coding device according to Claim 13 or Claim 14.

17. Information data transmission apparatus (48), characterized in that it comprises a coding device according to Claim 11 or Claim 12, an interleaver (20) able to permute the symbols of each code word $\underline{v} = \left(v^0, v^1, \ldots, v^{n-1}\right)$ so as to form a word to be transmitted

$$\underline{v}^* = \left(v^0, v^{q-1}, v^{2(q-1)}, \ldots, v^{(p-1)(q-1)}, v^1, v^q, v^{2q-1}, \ldots, v^{(p-1)(q-1)+1}, \ldots, v^{n-1}\right),$$

and a modulator (103) for modulating the symbols of said word to be transmitted $\underline{v}^*$.

18. Data reception apparatus (70), characterized in that it comprises a demodulator (106) for demodulating the received data so as to form interleaved received words

$$\underline{r}^* = \left(r^0, r^{q-1}, r^{2(q-1)}, \ldots, r^{(p-1)(q-1)}, r^1, r^q, v^{2q-1}, \ldots, r^{(p-1)(q-1)+1}, \ldots, r^{n-1}\right),$$

where q is an integer greater than 2 and equal to a power of a prime number, p an integer greater than 1, and $n = p(q-1)$, a deinterleaver (30) for permuting the symbols of each interleaved received word $\underline{r}^*$ so as to form a received word $\underline{r} = \left(r^0, r^1, \ldots, r^{n-1}\right)$, and a decoding device according to Claim 13 or Claim 14.

19. Non-removable data storage means, characterized in that it comprises computer program code instructions for executing the steps of a coding method according to any one of Claims 1 to 3, and/or of a decoding method according to any one of Claims 4 to 9, and/or of a communication method according to Claim 10.

20. Partially or totally removable data storage means, characterized in that it comprises computer program code instructions for executing the steps of a coding method according to any one of Claims 1 to 3, and/or of a decoding method according to any one of Claims 4 to 9, and/or of a communication method according to Claim 10.

21. Computer program, characterized in that it contains instructions such that, when said program controls a programmable data processing device, said instructions mean that said data processing device implements a coding method according to any one of Claims 1 to 3, and/or a decoding method according to any one of Claims 4 to 9, and/or a communication method according to Claim 10.